

identifying behaviour of said at least one computer indicative of malware infection.

3. A computer program product as claimed in claim 1, wherein said one or more
5 data I/O devices include one or more of:

- a floppy disk drive;
- a compact disk drive;
- a removable media drive; and
- a network interface card.

10

4. A computer program product as claimed in claim 1, wherein said device
disabling logic is operable upon detection of malware infection to disable at least one
data I/O device of at least one further computer.

15 5. A computer program product as claimed in claim 1, wherein said device
disabling logic is operable to require user confirmation prior to disabling said one or
more data I/O devices.

20 6. A computer program product as claimed in claim 1, wherein said device
disabling logic is operable to disable said one or more data I/O devices using an API
call to an operating system of said at least one computer.

7. A computer program product for controlling a computer, said computer
program product comprising:

25 device disabling logic operable upon receipt by a computer of a command
indicative of malware infection precautions being taken to disable operation of one or
more data I/O devices of said computer.

30 8. A computer program product as claimed in claim 7, wherein said one or more
data I/O devices include one or more of:

- a floppy disk drive;
- a compact disk drive;
- a removable media drive; and
- a network interface card.

9. A computer program product as claimed in claim 7, wherein said device disabling logic is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.

5

10. A computer program product for controlling a computer, said computer program product comprising:

user input logic operable to receive a user input indicative of activating precautions against a malware infection; and

10 device disabling logic operable upon receipt of said user input to disable operation of one or more data I/O devices of said at least one computer.

11. A computer program product as claimed in claim 10, wherein said one or more data I/O devices include one or more of:

15

a floppy disk drive;
a compact disk drive;
a removable media drive; and
a network interface card.

20

12. A computer program product as claimed in claim 10, wherein said device disabling logic is operable upon detection of malware infection to disable at least one data I/O device of at least one further computer.

25

13. A computer program product as claimed in claim 10, wherein said device disabling logic is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.

30

14. A method of protecting against malware infection, said method comprising the steps of:

detecting a malware infection of at least one computer; and
upon detection of said malware infection disabling operation of one or more data I/O devices of said at least one computer.

15. A method as claimed in claim 14, wherein detection of a malware infection is by one or more of:

positively identifying an item of malware upon said at least one computer; and
identifying behaviour of said at least one computer indicative of malware

5 infection.

16. A method as claimed in claim 14, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;
10 a compact disk drive;
a removable media drive; and
a network interface card.

17. A method as claimed in claim 14, wherein upon detection of malware
15 infection at least one data I/O device of at least one further computer is disabled.

18. A method as claimed in claim 14, wherein user confirmation is required prior to disabling said one or more data I/O devices.

20 19. A method as claimed in claim 14, wherein disabling said one or more data I/O devices uses an API call to an operating system of said at least one computer.

20. A method of protecting against malware infection, said method comprising the steps of:

25 upon receipt by a computer of a command indicative of malware infection precautions being taken disabling operation of one or more data I/O devices of said computer.

21. A method as claimed in claim 20, wherein said one or more data I/O devices
30 include one or more of:

a floppy disk drive;
a compact disk drive;
a removable media drive; and
a network interface card.

22. A method as claimed in claim 20, wherein disabling said one or more data I/O devices uses an API call to an operating system of said at least one computer.

5 23. A method of protecting against malware infection, said method comprising the steps of:

receiving a user input indicative of activating precautions against a malware infection; and

10 upon receipt of said user input disabling operation of one or more data I/O devices of said at least one computer.

24. A method as claimed in claim 23, wherein said one or more data I/O devices include one or more of:

15 a floppy disk drive;
a compact disk drive;
a removable media drive; and
a network interface card.

20 25. A method as claimed in claim 23, wherein upon detection of malware infection disabling at least one data I/O device of at least one further computer.

26. A method as claimed in claim 23, wherein disabling said one or more data I/O devices uses an API call to an operating system of said at least one computer.

25 27. Apparatus for protecting against malware infection, said apparatus comprising:

a malware infection detector operable to detect a malware infection of at least one computer; and

30 a device disabling unit operable upon detection of said malware infection to disable operation of one or more data I/O devices of said at least one computer.

28. Apparatus as claimed in claim 27, wherein said malware infection detector detects a malware infection by one or more of:

positively identifying an item of malware upon said at least one computer; and

identifying behaviour of said at least one computer indicative of malware infection.

29. Apparatus as claimed in claim 27, wherein said one or more data I/O devices
5 include one or more of:

- a floppy disk drive;
- a compact disk drive;
- a removable media drive; and
- a network interface card.

10

30. Apparatus as claimed in claim 27, wherein said device disabling unit is operable upon detection of malware infection to disable at least one data I/O device-of at least one further computer.

31. Apparatus as claimed in claim 27, wherein said device disabling unit is operable to require user confirmation prior to disabling said one or more data I/O devices.

32. Apparatus as claimed in claim 27, wherein said device disabling unit is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.

33. Apparatus for protecting against malware infection, said apparatus comprising:

25 a device disabling unit operable upon receipt by a computer of a command indicative of malware infection precautions being taken to disable operation of one or more data I/O devices of said computer.

34. Apparatus as claimed in claim 33, wherein said one or more data I/O devices
30 include one or more of:

- a floppy disk drive;
- a compact disk drive;
- a removable media drive; and
- a network interface card.

35. Apparatus as claimed in claim 33, wherein said device disabling unit is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.

5

36. Apparatus for protecting against malware infection, said apparatus comprising:

a user input unit operable to receive a user input indicative of activating precautions against a malware infection; and

10 a device disabling unit operable upon receipt of said user input to disable operation of one or more data I/O devices of said at least one computer.

37. Apparatus as claimed in claim 36, wherein said one or more data I/O devices include one or more of:

15 a floppy disk drive;
a compact disk drive;
a removable media drive; and
a network interface card.

20 38. Apparatus as claimed in claim 36, wherein said device disabling unit is operable upon detection of malware infection to disable at least one data I/O device of at least one further computer.

25 39. Apparatus as claimed in claim 36, wherein said device disabling unit is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.